



Warum Windows XP ??

- Stabil, hohe Funktionalität (Sicherheit, Multimedia, CD-RW-Support)
- Echtes Mehrbenutzersystem mit allen wichtigen Sicherheitsfunktionen von Windows-2000 (MultiUser, Sicherheitsrichtlinien, NTFS, ACL's)
- Automatische Systemupdates, automatische Sicherheitsüberprüfung
- Automatisches Checkpointing (System-Wiederherstellung)
- Sichere Defaults für Office, Mail und Internet
- Automatische Spam-Filter für E-Mail im JuNet (fz-juelich.de)
- Einfaches, aber effektives IP-Firewall bereits eingebaut
- Remote Desktop zur Fernwartung mit gesichertem Login



Betriebssystem einrichten

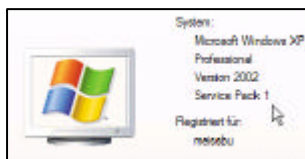
Arbeitsplatz Desktop Updates und Service Packs Fehlermeldung



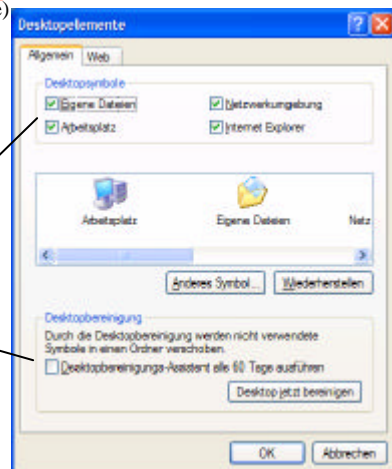
Windows-XP-Arbeitsplatz und Desktop

- **Zuallererst Service Packs einspielen:**

- Windows XP Service Pack 1 (xpsp1_de_x86.exe)
- Office Service Packs 1+2 (oxpsp1.exe, oxpsp2.exe)



- Danach gewohnte Desktop-Symbole einblenden und Desktopbereinigung ausschalten mit:
 - Desktop – RM* – Desktop – Desktop anpassen – Allgemein
 - * = rechte Maustaste drücken





Windows manuell auf den neuesten Stand bringen

Windows Update

- Vor der Installation von Patches und Updates: Anwendungen, **vor allem Virens Scanner und Firewall beenden!** System-Wiederherstellungspunkt erstellen.
- "Start – Hilfe und Support – Den Computer mit **Windows Update** auf dem neuesten Stand halten"
 - **Es ist eine Internet-Verbindung nach** (ggf. bei "Sichere Sites" eintragen!) <http://v4.windowsupdate.microsoft.com/de/default.asp?mode=updatecenter> erforderlich, und das Ausführen von ActiveX-Steuerelementen und Plugins sowie Scripting von Steuerelementen muß zugelassen sein!
- Updates suchen: Das lokale System wird analysiert, und es werden verfügbare Updates geordnet in drei Gruppen angeboten:
 - **Wichtige Updates und Service-Packs**
 - **Windows XP**
 - **Treiberupdates**
- Updates auswählen (zumindest die wichtigen Updates und Service Packs)
- Updates überprüfen und installieren – Jetzt installieren



Auswahl von Patches und Updates

Eine Aufgabe auswählen

Den Computer mit **Windows Update** auf dem neuesten Stand halten

Liste überprüfen, ungewünschte Updates entfernen, installieren

Internet Explorer

Ausführung von Software via ActiveX-Steuerelementen und Plugins zulassen?

Internet Explorer

Ein Skript greift auf Software (ein ActiveX-Steuerelement) auf dieser Seite zu (Ist sicher für Skripting markiert). Soll dies zugelassen werden?

Windows Update

Wichtige Updates und Service Packs

Wichtige Updates wurden bereits für die Installation ausgewählt.

Überprüfen Sie die Liste der wichtigen Updates. Sie können alle Elemente, die Sie nicht installieren möchten, entfernen.

Updates überprüfen und installieren

Gesamtzahl der ausgewählten Updates: (11)

018529: Kumulativer Patch für Internet Explorer, Juni 2003

Downloadgröße: 2,0 MB, < 1 Minute

Es wurden mehrere Sicherheitslücken in Microsoft® Internet Explorer entdeckt, durch die ein Angreifer auf Ihr Microsoft® Windows®-System zugreifen kann. Der Angreifer könnte dann verschiedene Aktionen durchführen, wie z. B. Programme auf den Computer ausführen, mit dem die Website dieses Antriebes besucht wurde. Diese Sicherheitslücke betrifft Computer mit Microsoft® Internet Explorer. (Die Sicherheitslücke besteht unabhängig davon, ob Sie Internet Explorer als Webbrowser verwenden oder nicht.) Durch die Installation dieses Updates von Microsoft können Sie Ihren Computer vor dieser Sicherheitslücke schützen. Nach der Installation dieses Updates müssen Sie gegebenenfalls den Computer neu starten. Weitere Informationen... (Diese Site ist möglicherweise in englischer Sprache.)

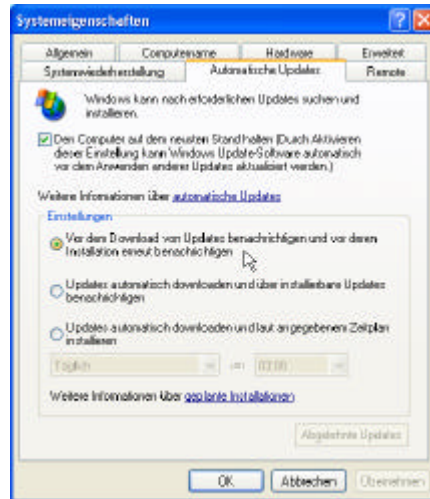
Dieses Element wurde gewählt.



System auf dem aktuellem Stand halten

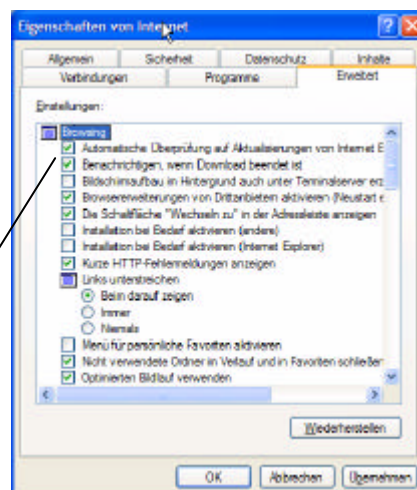
Automatische Updates

- Automatisches Windows-Update (unbedingt zu empfehlen) mit:
 - "Arbeitsplatz – RM – Eigenschaften – Automatische Updates – den Computer auf dem neuesten Stand halten" aktivieren
 - Vor dem Download und vor allem vor der Installation benachrichtigen (u.U. empfiehlt sich vorher die manuelle Erstellung eines Checkpoints. Manchmal muß das System nach der Installation auch neu gebootet werden)
 - ggf. auch nach Zeitplan installieren



Neue Versionen und Patches von Internet Explorer installieren

- werden auch mit Windows-Update installiert..... identischer Installationsumfang ???
- Internet Explorer-Symbol auf Desktop – RM – Eigenschaften
- Erweitert
- "Automatische Überprüfung auf Aktualisierungen von Internet Explorer" aktivieren





Downloads für Betriebssystem & Komponenten

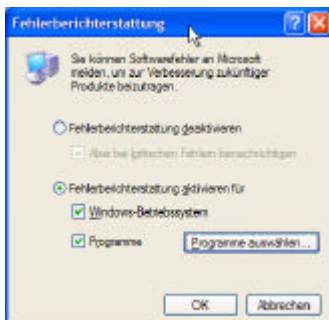
- Neue Betriebssystemversionen und Patches, Konfiguration:
 - [\\zelcds](#)
 - <http://support.microsoft.com/support/downloads>
- Office- und Explorer-Updates:
 - [\\zelcds.zel.kfa-juelich.de\Off97](#), [\\zelcds\Off2k](#)
 - [\\zelcds.zel.kfa-juelich.de\public\ie](#)
- Antiviren-Software:
 - [\\pcsrv.zam.kfa-juelich.de\public\nai\viruscan](#)
 - [\\pcsrv.zam.kfa-juelich.de\public\f-prot](#)
 - <http://www.fz-juelich.de/zam/net/security/software>
- AtGuard Firewall bzw. Norton Personal Firewall 2002
 - [\\zelcds.zel.kfa-juelich.de\atguard](#) [Symantec Live Update](#)
- Backup:
 - [\\pcsrv.zam.kfa-juelich.de\public\adsm](#) (Datensicherung)
 - 2 Disketten oder CD für PowerQuest [DeployCenter V5.01](#) (ZAM-Dispatch)



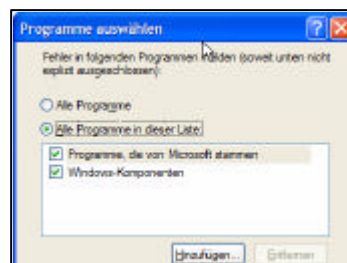
Fehlerberichte an Microsoft senden

Fehlerberichterstattung

- Arbeitsplatz – RM – Eigenschaften – Erweitert – Fehlerberichterstattung:



- Programme auswählen

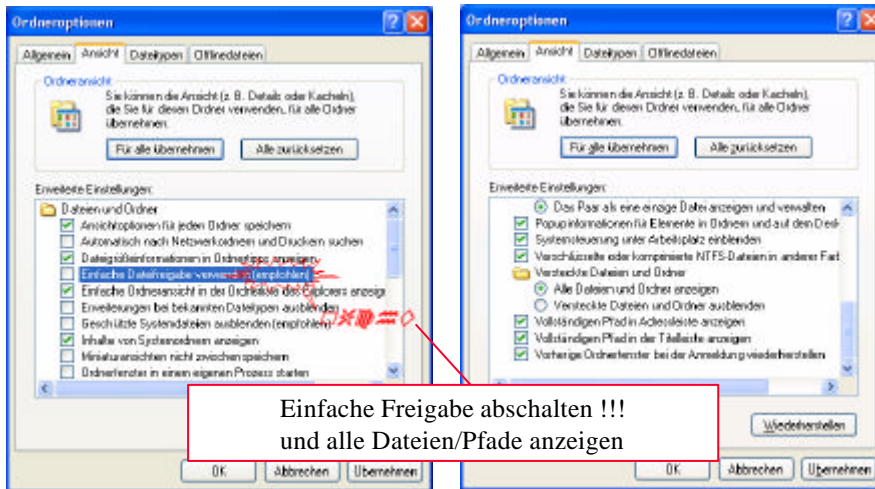


- Hier gegebenenfalls Programme anderer (seriöser) Hersteller zur Fehlerüberwachung hinzufügen



Ordneroptionen einrichten

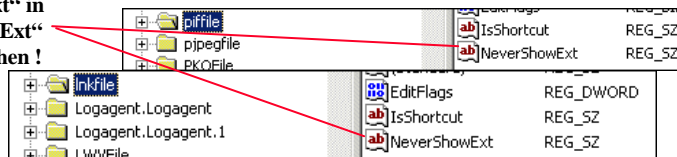
- Arbeitsplatz öffnen – Extras – Ordneroptionen - Ansicht



Erweiterungen bei bekannten Dateitypen *nicht* ausblenden

- Endungen auch für registrierte Dateien anzeigen. Beispiele:
 - **macrotest1.txt.rtf** → Word-Makro, angezeigt als **macrotest1.txt**
 - **Messung.gif.vbs** → Visual Basic Script, angezeigt als **Messung.gif**
- Grundsätzlich interpretiert beispielsweise Office eine Datei beim Öffnen nach ihrem Inhalt, nicht nach ihrer Endung !
 - Ein Makro in **macrotest1.doc**, umbenannt in **macrotest1.txt** wird beim Öffnen mit Word ausgeführt !

- Erweiterungen für bestimmte Dateien wie PIF, LNK etc. immer anzeigen: „NeverShowExt“ in „AlwaysShowExt“ ändern oder löschen !

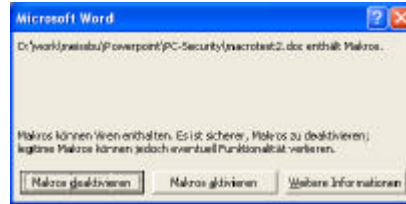


- Vorsicht beim Ausführen MIME-codierter EXE-Dateien (MHTML)



Makrovirus-Schutz

- Microsoft Word, Excel, Access, PowerPoint können Makro-Programme enthalten, die beim Öffnen des Dokuments automatisch gestartet werden
- Solche Programme haben vollen Zugriff auf alle Systemressourcen wie Laufwerke, Dateien, Programme, Registry, Benutzerdaten
- Deshalb mit "Extras - Optionen... – Sicherheit – Macro Sicherheit" die Sicherheitsstufe zumindest auf "Mittel" oder bei "Hoch" belassen
- Auch beim Öffnen eines Dokuments im Webbrowser (Plugin) funktioniert der Macro-Virenschutz:
- Vorsicht vor allem beim Öffnen von Dokumenten in der Anlage von E-Mails !!!



Solche Dokumente niemals ohne vorherigen Virenskan öffnen!!!



Sicherheitseinstellungen im Internet-Explorer

- Einstellungen „**Extras - Internetoptionen - Sicherheit**“

Internetzone: Voll qualifizierte Namen und Adressen außerhalb der eigenen IP-Domäne

Beispiele:
www.fz-juelich.de
zamprt.zam
aix.zam.kfa-juelich.de
www.microsoft.com

Lokales Intranet: Nicht weiter qualifizierte Namen, die um die eigenen IP-Domäne ergänzt werden

Beispiele:
localhost
www
\\zelcds\public

Eingeschränkte Sites: Sites, deren Besuch besonders hohe Sicherheit erfordert!

(am besten garnicht besuchen !!!)

Vertrauenswürdige Sites: Websites mit SSL (Secure Socket Layer)-Verschlüsselung des Datenverkehrs

Hiermit werden die persönlichen Einstellungen angepaßt



Einige „Glaubenssätze“ *)

- Das Intranet ist nicht viel sicherer als das Internet
- Man muß sich entscheiden, ob man nur mit ganz bestimmten Maschinen oder aber im weltweiten Netz arbeiten möchte
- Man muß entscheiden, ob man „sicher“ oder „komfortabel und schnell“ (nur mit Backup!) arbeiten möchte
- Bei jedem Mausklick nachzufragen verschiebt das Problem nur auf später
- Wer wirklich „sicher“ sein will, sollte seinen PC vom Netz ziehen und in einen Schrank schließen

*) Diese Sätze geben die persönliche Meinung des Verfassers wieder und sind keine offiziellen Aussagen des Forschungszentrums Jülich oder des Instituts für Angewandte Mathematik ZAM. Vielleicht sind sie sogar falsch- aber das muß jeder für sich entscheiden !!!



Was kann der Internet-Explorer ?

- Der Internet-Explorer interpretiert die von einem Webserver heruntergeladenen (D)HTML-Dateien (Webseiten) und stellt sie dar
- Er liefert auf Anfrage des Servers Informationen über den Benutzer (Adressen, Referer, Cookies, MIME-Types) und dessen Browsingprofil („privacy“)
- Er führt die in der HTML-Seite eingebetteten Scripts (JavaScript oder VBScript) in einer (hoffentlich) abgesicherten (?) Umgebung aus (Script Host)
- Er lädt automatisch ActiveX-Steuerelemente vom Webserver und/oder führt diese lokal auf dem PC aus (C:\%WINDIR%\Downloaded program files)
- Er lädt bei Bedarf (gesteuert durch den MIME-Typ des angeforderten Dokuments) Plugin-Programme und zeigt deren Ergebnisse als integralen Bestandteil der gerade dargestellten Webseite an (Plugin-Fehler ?)
- Er läßt sich als Automation Object beliebig neu instanzieren und durch Scripting fernsteuern (auch völlig unsichtbar im Hintergrund)



„Internetoptionen - Sicherheit - Stufe anpassen“ (1)

- Auch sichere ActiveX-Controls sind nicht wirklich sicher!
- Das auf jeden Fall verhindern!
- Manchmal braucht man die einfach (z.B. Acrobat-Reader)
- Hängt vom Vertrauen in den Serverbetreiber ab!
- Auf keinen Fall, zu gefährlich!
- Entweder immer fragen oder nur im Intranet den aktuellen Namen und Paßwort benutzen

The screenshot shows the 'ActiveX-Steuerelemente und Plugins' section of Internet Options. It lists several categories with their respective security settings:

- ActiveX-Steuerelemente ausführen, die für Scripting sicher sind:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- ActiveX-Steuerelemente initialisieren und ausführen, die nicht sicher sind:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- ActiveX-Steuerelemente und Plugins ausführen:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Vom Administrator genehmigt
- Download von signierten ActiveX-Steuerelementen:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Download von unsignierten ActiveX-Steuerelementen:**
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Benutzerauthentifizierung:**
 - Anmeldung
 - Anonyme Anmeldung
 - Automatische Anmeldung mit aktuellem Benutzernamen
 - Automatisches Anmelden nur in der Intranetzone
 - Nach Benutzername und Kennwort fragen



„Internetoptionen - Sicherheit - Stufe anpassen“ (2)

- Cookies sind harmlos (können aber vom Serverbetreiber zum Erstellen von Nutzerprofilen benutzt werden)
- Ab und zu muß man mal eine Datei herunterladen.
- Schriftarten (Fonts) sind wohl unproblematisch und sorgen für korrekte Darstellung
- Java sollte mit hoher Sicherheit immer gut genug funktionieren. Individuelle Einstellungen sind aber mit „Benutzerdefiniert“ möglich

The screenshot shows the 'Content Advisor' section of Internet Options. It lists several categories with their respective security settings:

- Cookies:**
 - Cookies annehmen, die gespeichert sind
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Cookies pro Sitzung annehmen (nicht gespeichert)
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Download:**
 - Dateidownload
 - Aktivieren
 - Deaktivieren
 - Schriftartdownload
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Microsoft VM:**
 - Java-Einstellungen
 - Benutzerdefiniert
 - Hohe Sicherheit
 - Java deaktivieren
 - Mittlere Sicherheit
 - Niedrige Sicherheit



„Internetoptionen - Sicherheit - Stufe anpassen“ (3)

- **Active Scripting ist nicht sicher.**
Aber ohne kann man kaum auskommen. Das ist sicher!
- Kaum gebraucht, daher nachfragen!
- Kaum benutzt, nachfragen!
- Sollte eigentlich kein Server tun, also abschalten!
- Wird auch von Microsoft immer abgeschaltet!
- Nur wenn man sich sicher ist, deshalb nachfragen!

Scripting

- Active Scripting
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Einfügeoperationen über ein Skript zulassen
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Scripting von Java-Applets
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Verschiedenes
 - Auf Datenquellen über Domänengrenzen hinweg zugreifen
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
 - Dauerhaftigkeit der Benutzerdaten
 - Aktivieren
 - Deaktivieren
 - Installation von Desktopobjekten
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung



„Internetoptionen - Sicherheit - Stufe anpassen“ (4)

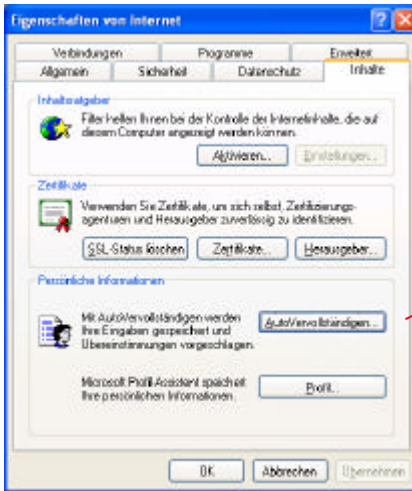
- Nur, wenn man dem Server vertraut. Deshalb fragen!
- Unbedingt nachfragen, damit man es überhaupt merkt!
- Da kann zwar jeder mitlesen, aber ohne geht's kaum (besser wäre natürlich SSL)!
- Unkritisch, deshalb aktiviert!
- Was immer das heißt!

- Programme und Dateien in einem IFRAME starten
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Subframes zwischen verschiedenen Domänen bewegen
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Unverschlüsselte Formular Daten übermitteln
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Ziehen und Ablegen oder Kopieren und Einfügen von Dateien
 - Aktivieren
 - Deaktivieren
 - Eingabeaufforderung
- Zugriffsrechte für Softwarechannel
 - Hohe Sicherheit
 - Mittlere Sicherheit
 - Niedrige Sicherheit

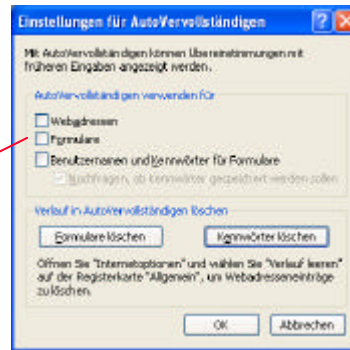


Speichern von Formulardaten vermeiden

- Internetooptionen - Inhalte



- keine Formulardaten und
- keine Kennwörter speichern



Benutzerkonten einrichten

Kontotypen, Administrator-Konto

Konten-Richtlinien

Benutzerkonten

Remote Desktop



Paßwortschutz

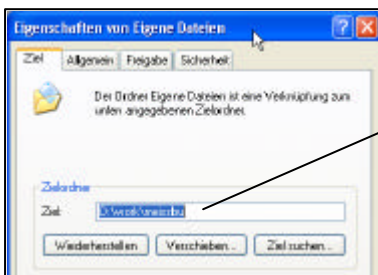
- BIOS-Paßwort verhindert unbefugtes Booten des Systems:
 - Administratives Paßwort zum Schutz der BIOS-Konfiguration
 - Benutzerpaßwort zum Schutz des Windows -Betriebssystems
- Benutzer individuell mit eigenen Profilen einrichten:
 - NT/2k: „Programme - Verwaltung – Benutzermanager/Computerverwaltung“
 - Win95/98/XP: „Start - Systemsteuerung - Benutzerkonten bzw. Kennwörter“
- Anonyme oder wohlbekannte Benutzernamen vermeiden:
 - Gast / Guest / *USR_Computername* für anonymen Webzugang, Anonymous FTP
 - Administrator unbedingt mit Paßwort einrichten
- Paßwortverschlüsselung für Shares (Windows 98+ und NT+):
 - Paßwort geht bei jedem „Laufwerk verbinden“ über das Netz
 - Paßwortverschlüsselung auch bei Zugriff auf Samba-Server benutzen
 - Keine "einfachen" Freigaben benutzen
- Bildschirmschoner mit Paßwortschutz aktivieren (ca. 5..10 Minuten)



Vorderfinierte Kontentypen

- Berechtigungen für Kontotypen „Computeradministrator“ und „Eingeschränkt“
- Eingeschränkte Benutzer haben nur Zugriff auf „Eigene Dateien“ oder Dateien im Arbeitsplatz-Ordner „Gemeinsame Dokumente“

	Computer-administrator	Eingeschränkt
Installieren von Programmen und Hardware	✓	
Vornehmen von Änderungen am System	✓	
Zugriffs- und Leseberechtigung für alle nicht privaten Dateien	✓	
Erstellen und Löschen von Benutzerkonten	✓	
Ändern von Konten anderer Personen	✓	
Ändern des eigenen Kontonamens oder -typs	✓	
Ändern des eigenen Bildes	✓	✓
Erstellen, Ändern oder Entfernen des eigenen Kennworts	✓	✓



- Ordner „Eigene Dateien“ wenn möglich mit: „Eigene Dateien – RM – Eigenschaften – Verschieben“ auf separate Partition verschieben



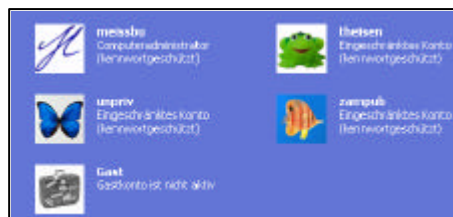
Administrator-Kennwort einrichten

- Der erste Benutzer, der während der Systeminstallation eingerichtet wird, erhält automatisch Administratorrechte
- Der Benutzer „Administrator“ ist jedoch auf allen Windows-XP-Systemen per Default zusätzlich **ohne Paßwort** eingerichtet
 - Siehe: Arbeitsplatz – RM – Eigenschaften – Erweitert – Benutzerprofile – Einstellungen
- Das Administrator-Konto ist für die Anmeldung nicht sichtbar!
- Zum Setzen eines Passwortes Rechner mit F8 im abgesicherten Mode hochfahren
- Mit "Start – Systemsteuerung – Benutzerverwaltung" ein Paßwort für "Administrator" einrichten



Benutzerkonten einrichten oder ändern

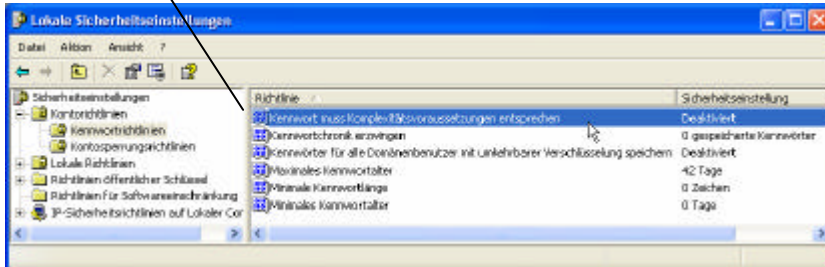
- Start – Systemsteuerung – Benutzerkonten
 - Konto ändern
 - Neues Konto erstellen
 - Art der Benutzeranmeldung ändern
- Alle Konten mit Paßwort schützen !
- Erster Benutzer ist automatisch Systemadministrator
- Eingeschränktes Konto für Normalbenutzer
- Gastkonto nicht aktivieren (gilt nur für interaktives Login !)
- Willkommenseite oder klassische Anmeldung (sicherer) verwenden
- Schnelle Benutzerumschaltung möglichst vermeiden





Kennwort-Richtlinien

- Diese definieren den Default beim Einrichten eines neuen Benutzers
 - Start – Systemsteuerung – Verwaltung – Lokale Sicherheitsrichtlinie
 - Sicherheitseinstellungen – Kontorichtlinien – Kennwortrichtlinien
- Je nach Sicherheitsbedarf sinnvolle Werte einsetzen (zumindest minimale Kennwortlänge und ggf. Kennwortalter)
- Aktivieren



Eigene Netzwerkkennwörter verwalten

- Start – Systemsteuerung – Benutzerkonten – Konto ändern – Konto auswählen – Verwandte Aufgaben – Eigene Netzwerkkennwörter verwalten
- Kennwörter für Domänenanmeldung und Freigaben im Netz





Remoteunterstützung und Remote Desktop

- Zugriff (Chat mit Anzeige des Bildschirms) nach Einladung über Windows Messenger oder Outlook
- Voller Zugriff auf laufende Windows-Sitzung und alle Systemressourcen



Sicherheitswerkzeuge von Microsoft

MBSA

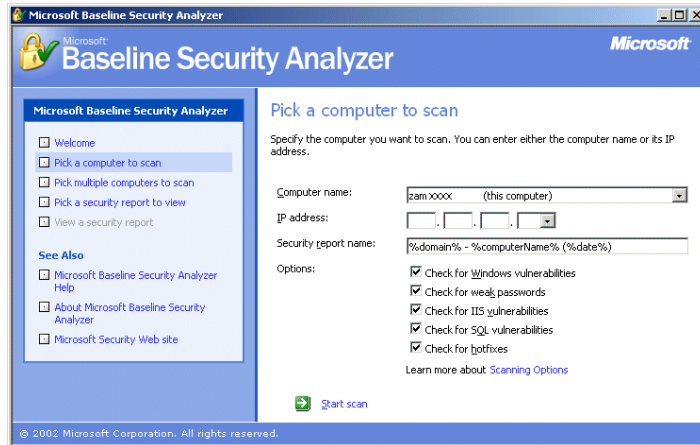
LockDownTool

URLScan



System mit MBSA überprüfen

- Der **Microsoft Baseline Security Analyzer** analysiert die Sicherheit des
 - (lokalen) Betriebssystems, Update-Level, Sicherheitspatches, Passwörter
 - des Internet Information Servers (IIS) und seiner Konfiguration



Security Report: Systemkonfiguration

- Windows-Status, Patches, Sicherheitsupdates
- Null-Session Enumeration* erlaubt anonymen Zugriff auf Benutzerinformationen
- Zahl der Benutzer mit Administratorrechten
- Passwort-Richtlinie
- Passwort-Qualität
- Sicherheit des Dateisystems





Null-Session Enumeration (Anonyme Aufzählung)

- Erlaubt **netzwerkweiten, anonymen** Zugriff auf Benutzernamen, Freigaben und Kontenrichtlinien.
- Diese Einstellung ist **Default** bei allen Windows-Systemen!
- Liefert wichtige Informationen für Hacker-Angriffe.

Baseline Security Analyzer

Restrict Anonymous Users

Issue

The **RestrictAnonymous** registry setting controls the level of enumeration granted to an anonymous user. If **RestrictAnonymous** is set to 0 (that is, the default setting), any user can obtain system information, including: user names and details, account policies, and share names. Anonymous users can use this information in an attack against your system. The list of user names and share names could help potential attackers identify who is an administrator, which computers have weak account protection, and which computers share information with the network.

Solution

To restrict anonymous connections from accessing this system information, change the **RestrictAnonymous** security settings. You can do this through the Security Configuration Manager snap-in (setting is defined in the Local Policies portion of the default security templates), or through a registry editor. You can change the registry setting from 0 to 1 in Microsoft Windows NT 4.0, or from 0 to 1 or 2 in Windows 2000:

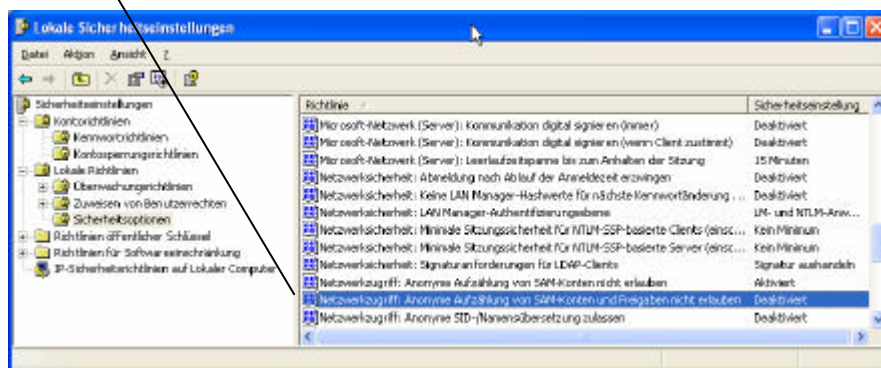
- 0 - None. Rely on default permissions
- 1 - Do not allow enumeration of Security Accounts Manager (SAM) accounts and names
- 2 - No access without explicit anonymous permissions (not available on Windows NT 4.0)

Caution: Before you set this value to 2, see article Q246261, "How to Use the RestrictAnonymous Registry Value in Windows 2000." It is recommended that you do not set this value to 2 on Domain Controllers in mixed-mode environments (e.g., networks with downlevel clients). In addition, client machines with **RestrictAnonymous** set to 2 should not take on the role of master browser.



Anonyme Aufzählung verhindern

- Start – Systemsteuerung – Verwaltung – Lokale Sicherheitsrichtlinie
- Lokale Richtlinie – Sicherheitsoptionen
 - "Netzwerkzugriff: Anonyme Aufzählung nicht erlauben" aktivieren





Internet Information Server

- Version und Sicherheitspatches
- Webserver-Konfiguration (Lockdown-Tool)
- Zugriff auf Beispielsanwendungen (Risiko, Default!)
- Parent Path (dot-dot-vulnerability)
- Zugriff auf gefährdete Script-Directories
- Remote IIS-Administrator

Internet Information Services (IIS) Scan Results

Vulnerabilities		
Score	Issue	Result
✗	IIS Hotfixes	1 missing hotfixes were found. What was scanned Result details How to correct this
✗	IIS Lockdown Tool	The IIS Lockdown tool has not been run on the machine. What was scanned How to correct this
✗	Sample Applications	Some IIS sample applications are installed. What was scanned Result details How to correct this
✗	Parent Paths	Parent paths are enabled in some web sites and/or virtual directories. What was scanned Result details How to correct this
✘	Mscad and Scripts Virtual Directories	MSADC virtual directory was found under the default web site. Scripts virtual directory was found under the default web site. What was scanned How to correct this
✓	IIS Admin Virtual Directory	IISADMPWD virtual directory is not present. What was scanned

Additional System Information		
Score	Issue	Result
✘	IIS Logging Enabled	Some web or FTP sites are not using the recommended logging options. What was scanned Result details How to correct this
✘	Domain Controller Task	IIS is not running on a domain controller.



Security Report: Anwendungen

- Hier werden veränderte, auch sicherere Einstellungen angezeigt!

Microsoft Baseline Security Analyzer

Internet Explorer zones do not have secure settings for some users.

Result Details

Note that custom settings may be more secure than recommended settings.

Score	User	Zone	Level	Recommended Level
✗	ZAM016\ymeissbu	Lokales Intranet	Custom	Medium
✗	ZAM016\ymeissbu	Vertrauenswürdiges Sites	Custom	Medium
✗	ZAM016\ymeissbu	Internet	Custom	Medium
✗	ZAM016\ymeissbu	Eingeschränkte Sites	Custom	High

SQL Server Scan Results

Score	Issue	Result
✗	SQL Server Status	SQL Server is not installed on this computer.

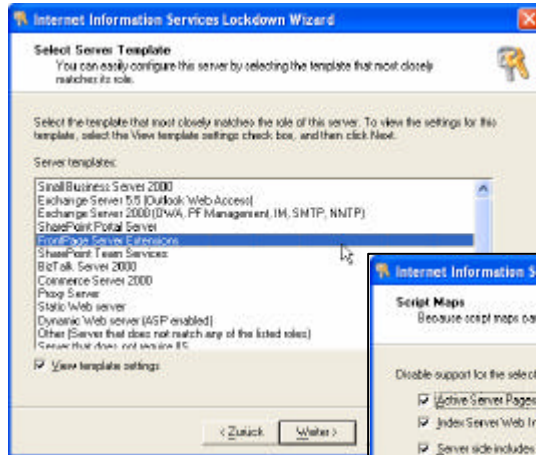
Desktop Application Scan Results

Vulnerabilities		
Score	Issue	Result
✘	IE Zones	Internet Explorer zones do not have secure settings for some users. What was scanned Result details How to correct this
✘	Outlook Zones	Microsoft Outlook 2002: Some security issues were found. What was scanned Result details How to correct this
✓	Macro Security	4 Microsoft Office product(s) are installed. No issues were found. What was scanned Result details

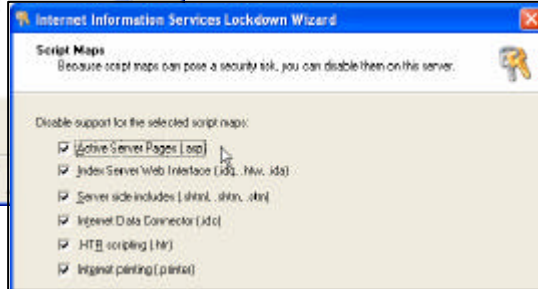
• Ergebnisse mit "What was scanned" und "Result details" überprüfen!



IIS Lockdown Tool (iislockd.exe)

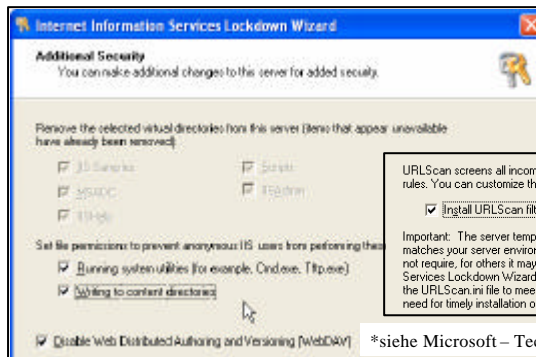


- Sichern des Internet Information Servers (Webserver, FTP)
- Deaktivieren von (manchen) Script Maps



weitere Sicherheitseinstellungen

- Entfernen der *virtuellen* Directories für Beispielanwendungen und Remote-Management des Servers
- Verhindern der Ausführung von Systemprogrammen im Webserver
- Deaktivieren von WebDAV und MSADC



- Installation von URLScan*-Filtern (Konfiguration in %sysroot%\urlscan.ini)

URLScan screens all incoming requests to this server and filters them based on a set of rules. You can customize the rules based on the role of your server.

Install URLScan filter on the server

Important: The server template that you've selected chooses a filter configuration that most closely matches your server environment. For some server environments, it may enable functionality you do not require, for others it may disable functionality you need. After completing the Internet Information Services Lockdown Wizard, Microsoft recommends you read the URLScan documentation, and tune the URLScan.ini file to meet your specific needs. In addition, remember that no tool replaces the need for timely installation of service packs and hotfixes. For more information, click Help.



Netzicherheit

Freigaben (NetBIOS)

TCP/IP-Filterung

Internet-Verbindungsfirewall

Dienste



Zugriffe auf Freigaben

- Geschützte Freigaben nur möglich, wenn die „Einfache Freigabe“ abgeschaltet ist !

The image displays two screenshots of the Windows XP 'Eigenschaften von Temp' dialog box. The left screenshot shows the 'Freigabe' tab where the 'Diesen Ordner freigeben' option is selected. The 'Freigabename' field contains '\$Temp'. A red arrow points to this field, and a callout box states 'Freigabennamen mit \$ verstecken !'. The right screenshot shows the 'Sicherheit' tab, listing users: Administratoren (ZAM227-Administratoren), Benutzer (ZAM227-Benutzer), ERSTELLER-BESITZER, Inesibu (ZAM227-inesibu), and SYSTEM. A callout box points to 'Benutzer (ZAM227-Benutzer)' and says 'andere Benutzer nur Leserechte'. The permissions table below shows 'Lesen' is checked for the selected user.

Berechtigungen für Inesibu	Zulassen	Verweigern
Vollzugriff	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ändern	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen, Ausführen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Ordnerinhalt auflisten	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Lesen	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Schreiben	<input checked="" type="checkbox"/>	<input type="checkbox"/>



Effektive Besitzer- und Benutzerrechte

Besitzrechte hier ändern

Erweiterte Sicherheitseinstellungen für Temp

Berechtigungen | Überwachung | Besitzer | Effektive Berechtigungen

Sie können die Besitzrechte für ein Element übernehmen, wenn Sie über die erforderlichen Rechte verfügen.

Aktueller Besitzer dieses Elements:
meissbu [ZAM227\meissbu]

Besitzer ändern auf:

Name
 Administratoren (ZAM227\Administratoren)
 meissbu (ZAM227\meissbu)

Effektive Berechtigungen:

Die folgende Liste zeigt die Berechtigungen, die der ausgewählten Gruppe oder gespeichert wurden, basierend auf allen relevanten Berechtigungen an.

Gruppen- oder Benutzernamen:
meissbu

Effektive Berechtigungen:

- Vollzugriff
- Ordner durchsuchen / Datei ausführen
- Ordner ausführen / Daten lesen
- Attribute lesen
- Erweiterte Attribute lesen
- Dateien erstellen / Daten schreiben
- Ordner erstellen / Daten anhängen
- Attribute schreiben
- Erweiterte Attribute schreiben
- Unterverzeichnisse und Dateien löschen
- Löschen
- Berechtigungen lesen
- Berechtigungen ändern
- Besitzrechte übernehmen

Berechtigungen | Überwachung | Besitzer | Effektive Berechtigungen

Weitere Informationen über spezielle Berechtigungen erhalten Sie, indem Sie die Berechtigung auswählen und auf "Bearbeiten" klicken.

Typ	Name	Berechtigung	Geht auf	Übernehmen für
Zulass.	meissbu (ZAM227)	Vollzugriff	nicht zugeordnet...	Dieses Ordner, Unt...
Zulass.	Administratoren (Z...	Vollzugriff	übergeordnet...	Dieses Ordner, Unt...
Zulass.	Benutzer (ZAM22...	Speziell	übergeordnet...	Dieses Ordner, Unt...
Zulass.	Benutzer (ZAM22...	Lesen, Ausfö...	übergeordnet...	Dieses Ordner, Unt...
Zulass.	ERSTELLER-BES...	Vollzugriff	übergeordnet...	Nur Unterverzeich...
Zulass.	meissbu (ZAM227)	Vollzugriff	übergeordnet...	Nur diesen Ordner
Zulass.	SYSTEM	Vollzugriff	übergeordnet...	Dieses Ordner, Unt...

Hinzufügen... Bearbeiten... Entfernen

Berechtigungen übergeordneter Objekte auf untergeordnete Objekte, sofern anwendbar, vererben. Diese mit den hier definierten Einträgen mit einberechnen.

J.Meißburger, FZJ -ZAM

Seite 41



Grundregeln für Freigaben (Shares)

- Nie das Root-Verzeichnis (ganze Festplatte oder Partition) freigeben !
- Keine Freigaben ohne, mit trivialen oder mit unverschlüsselten (Win95) Paßwörtern
- Freigaben durch angehängtes „\$“ im Netz unsichtbar machen
- Zugriffe auf kritische Freigaben gegebenenfalls loggen (ACL's)
- Für Standalone-Systeme auf administrative Freigaben verzichten
 - In
HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\LA
NMANSERVER\PARAMETERS
 - den REG_DWORD-Wert für "AutoShareWKS" von 1 auf 0 setzen !
 - die IPC\$-Freigabe für Remote Pipes bleibt erhalten
- Mit "Start – Ausführen" von "cmd net share" offene Shares überprüfen

J.Meißburger, FZJ -ZAM

Seite 42



Freigabe und Webfreigabe von Ordnern

- Share-Freigabe für den Zugriff aus dem Netz (Netzlaufwerk) mit Hilfe der „NETBIOS -Dienste“ (über IP) im Microsoft Netzwerk
- Administrative Shares werden automatisch bei Systeminstallation (NT) eingerichtet (werden z.B. für die Task-to-Task-Kommunikation benutzt)
 - Windows NT: ADMIN\$. IPC\$. C\$. D\$..... Für administrativen Zugriff
 - aber auch: Taskplaner (Outlook), Drucker, Webseiten (IIS oder Peer Web Server)
- Überprüfen mit
 - „net share“ bzw.
 - „net view \\{rechnername}“
- Web-Freigaben:
 - mit dem Internet-Dienst-Manager überprüfen (anonym/NT-Anmeldung)
 - Aliasnamen benutzen: C:\InetPub\wwwroot\cgi-bin ☒ http://webserver/bin
 - Zugriffsrechte entsprechend setzen (nur Lesen, Scripte nur ausführen etc.)
 - Anonymen Zugriff erlauben oder Windows-Authentisierung

```
C:\>net share

Name                Ressource            Beschreibung
-----
ADMIN$              C:\WINNT             Remote-Admin
IPC$                 C:\                  Remote-IPC
C$                   D:\                  Standardfreigabe
D$                   P:\                  Standardfreigabe
P$                   P:\                  Standardfreigabe

Der Befehl wurde erfolgreich ausgeführt.
```

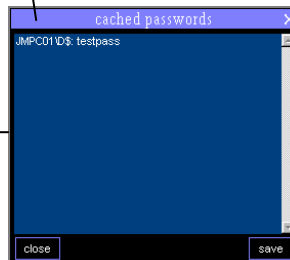
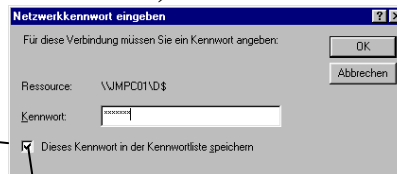
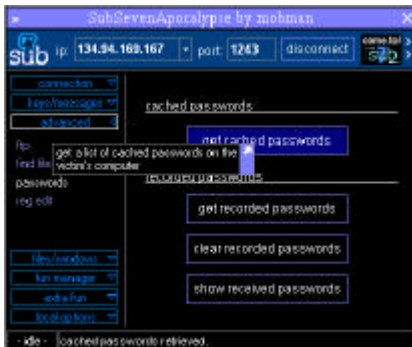


Speichern von NETBIOS-Paßwörtern (deshalb kein Win95 mehr !)

- Keine Kennwörter in der Kennwortliste

C:%WINDIR%\{userid}.pwl

abspeichern !

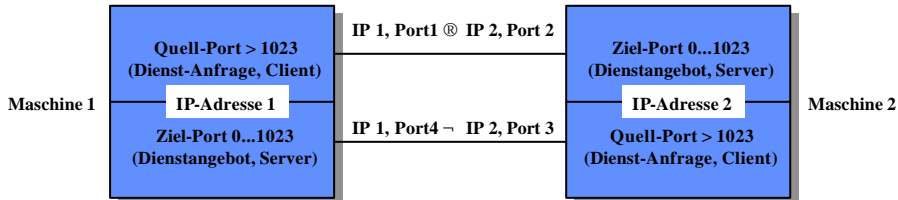


- Ein Trojaner könnte sie ganz leicht auslesen und mißbrauchen!



Das Prinzip der IP-Kommunikation

- Ein IP-Verbindung zwischen zwei Maschinen wird über "IP-Sockets" mit Hilfe der WinSock-Schnittstelle (WINSOCK.DLL) hergestellt:



- Ein Server bietet Dienste im Netz an, indem ein Programm (ein "Dienst") auf einem ganz bestimmten IP-Port (TCP oder UDP) "lauscht"

PortNumbers

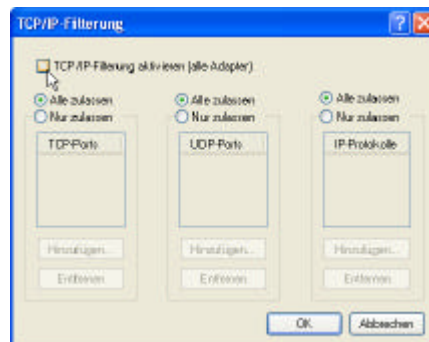
- Ein Client versucht
 - sich mit diesem Port zu verbinden ("SYNC") und dann über die stehende Verbindung Daten auszutauschen (verbindungsorientiert, TCP)
 - oder einfach Pakete an den Port zu senden und zu hoffen, daß diese ankommen (verbindungslos, UDP)



TCP/IP-Filterung

- Netzwerkumgebung – RM – Eigenschaften – LAN-Verbindung – RM – Eigenschaften
- Internetprotokoll (TCP/IP) – Allgemein – Erweitert – Optionen – TCP/IP-Filterung – Eigenschaften

- Hier können IP-Protokolle
 - <http://www.iana.org/assignments/protocol-numbers>
- und Port Numbers (Dienste)
 - <http://www.iana.org/assignments/port-numbers>
- eingerichtet werden, die den lokalen Rechner erreichen dürfen



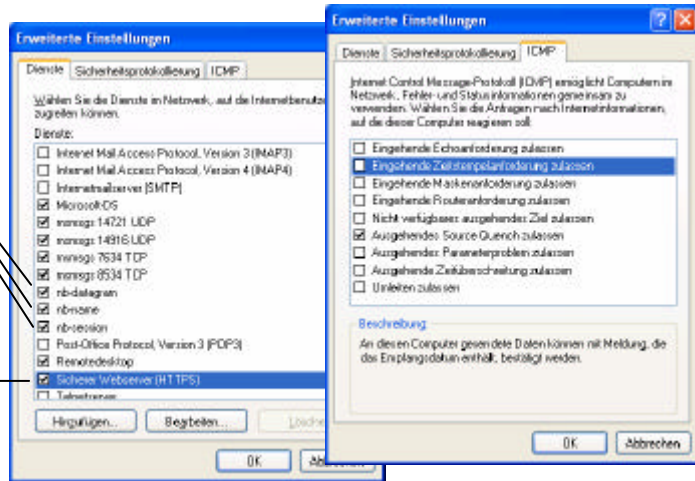


Internetverbindungsfirewall

- Netzwerkumgebung – RM – Eigenschaften – LAN-Verbindung – RM – Eigenschaften – Erweitert – Internetverbindungsfirewall aktivieren

• Für Zugriff auf Freigaben (Shares) aktivieren !

• HTTPS (SSL) Webserver aktivieren



Welche Dienste biete ich an und wer ist mit meinem System verbunden ?

- Mit "netstat -a | more" in einer DOS-Box werden die auf zam125 aktiven Ports und Verbindungen angezeigt:

Annotation	Protocol	Local Address	Foreign Address	State
NETBIOS-Verbindung zu einem lokalen Share	TCP	zam125-1036	0.0.0.0	LISTENING
	TCP	zam125-1038	0.0.0.0	LISTENING
Verbindung zum Mailserver des FZJ	TCP	zam125-1202	0.0.0.0	LISTENING
	TCP	zam125-1026	0.0.0.0	LISTENING
Aktive Verbindungen zum Webserver www.microsoft.com	TCP	zam125-1026	localhost:1036	ESTABLISHED
	TCP	zam125-1030	0.0.0.0	LISTENING
Lokale genutzte Dienste	TCP	zam125-1034	0.0.0.0	LISTENING
	TCP	zam125-1036	localhost:1026	ESTABLISHED
UDP-Dienste, die im Netz angeboten werden	TCP	zam125-1076	0.0.0.0	LISTENING
	TCP	zam125-137	0.0.0.0	LISTENING
	TCP	zam125-138	0.0.0.0	LISTENING
	TCP	zam125-nbssession	0.0.0.0	LISTENING
	TCP	zam125-nbssession	zam486.zam.kfa-juelich.de:4704	ESTABLISHED
	TCP	zam125-1038	zam079-a.fz-juelich.de:143	ESTABLISHED
	TCP	zam125-1201	207.46.131.137:80	ESTABLISHED
	TCP	zam125-1202	207.46.131.137:80	ESTABLISHED
	UDP	zam125-portmap	**:	**:
	UDP	zam125-135	**:	**:
	UDP	zam125-1033	**:	**:
	UDP	zam125-1076	**:	**:
	UDP	zam125-nbname	**:	**:
	UDP	zam125-nbdatagram	**:	**:



Dienste

- Welche werden unbedingt, welche manchmal, welche überhaupt nicht benötigt ?
- Mit "Start – Verwaltung – Dienste" überprüfen. Bei Auswahl eines Dienstes wird links eine ausführliche Beschreibung angezeigt.
- Mit "msconfig" die Nicht-Microsoft-Dienste anzeigen
- Ggf. mit Hilfsprogrammen wie "procxp" oder "prcview" die laufenden Prozesse anzeigen
- Versuchsweise voraussichtlich nicht benötigte Dienste nacheinander auf Startart "Manuell" umschalten und beenden
- Zum sicheren Testen mit "Arbeitsplatz – RM – Eigenschaften – Hardware – Hardwareprofile" das aktuelle Profil kopieren und in diesem Testprofil die Änderungen vornehmen



XP-Dienste (1)

1	Ablagemappe	21	Geschützter Speicher
2	Anmeldedienst	22	HID Input Service
3	Anwendungsverwaltung	23	Hilfe und Support
4	Arbeitsstationsdienst	24	IBM PM Service
5	Ati HotKey Poller	25	IIS Admin
6	Automatische Updates	26	IMAPI CD-Burning COM Service
7	AVSync Manager	27	Indexdienst
8	Cisco Systems, Inc. VPN Service	28	Infrarotüberwachung
9	COM+-Ereignissystem	29	Intelligenter Hintergrundübertragungsdienst
10	COM+-Systemanwendung	30	Internetverbindungsfirewall/Gemeinsame Nutzung der Internetverbindung
11	Computerbrowser	31	IPSEC-Dienste
12	Designs	32	Kompatibilität für schnelle Benutzerumschaltung
13	DHCP-Client	33	Konfigurationsfreie drahtlose Verbindung
14	Distributed Transaction Coordinator	34	Kryptografiedienste
15	DNS-Client	35	Leistungsdatenprotokolle und Warnungen
16	Druckwarteschlange	36	Machine Debug Manager
17	Ereignisprotokoll	37	McShield
18	Fehlerberichterstattungsdienst	38	MS Software Shadow Copy Provider
19	FTP-Publishing	39	MySql
20	Gatewaydienst auf Anwendungsebene	40	Nachrichtendienst



XP-Dienste (2)

41	NetMeeting-Remotedesktop-Freigabe	61	Shellhardwareerkennung
42	Netzwerk-DDE-Dienst	62	Sicherheitskontenverwaltung
43	Netzwerk-DDE-Serverdienst	63	Sitzungs-Manager für Remotedesktophilfe
44	Netzwerkverbindungen	64	Smartcard
45	NLA (Network Location Awareness)	65	Smartcard-Hilfsprogramm
46	Norton Personal Firewall Accounts Manager	66	SSDP-Suchdienst
47	Norton Personal Firewall Proxy Service	67	Systemereignisbenachrichtigung
48	Norton Personal Firewall Service	68	Systemwiederherstellungsdienst
49	NT-LMSicherheitsdienst	69	Taskplaner
50	Plug & Play	70	TCP/IP-Druckserver
51	QCONSVC	71	TCP/IP-NetBIOS-Hilfsprogramm
52	QoS-RSVP	72	Telefonie
53	RAS-Verbindungsverwaltung	73	Telnet
54	Remoteprozessaufruf (RPC)	74	Terminaldienste
55	Remote-Registrierung	75	Treibererweiterungen für Windows-Verwaltungsinstrumentation
56	Routing und RAS	76	TSM Client Acceptor zam016
57	RPC-Locator	77	TSM Remote Client Agent
58	Sekundäre Anmeldung	78	Überwachung verteilter Verknüpfungen (Client)
59	Seriennummer der tragbaren Medien	79	Universeller Plug & Play-Gerätehost
60	Server	80	Unterbrechungsfreie Stromversorgung



XP-Dienste (3)

- Start – Systemsteuerung – Verwaltung – Dienste
- Startart "Automatisch": Wird bei Systemstart gestartet
- Startart "Manuell": Wird bei Bedarf von Programmen gestartet

Unbedingt erforderlich

meist erforderlich

81	Upload-Manager
82	Verwaltung für automatische RAS-Verbindung
83	Verwaltung logischer Datenträger
84	Verwaltungsdienst für die Verwaltung logischer Datenträger
85	Volumeschattenkopie
86	Warndienst
87	WebClient
88	Wechselmedien
89	Windows Audio
90	Windows Installer
91	Windows-Bilderfassung (WIA)
92	Windows-Verwaltungsinstrumentation
93	Windows-Zeitgeber
94	WMI-Leistungsadapter
95	WWW-Publishing



Zur Sicherheit des Internet Information Server IIS

- FTP und Remote Administration deaktivieren
- Webserver nur wenn unbedingt erforderlich auf Standardports (80, 8081, 8080 etc.) aktivieren
- Standarddokument definieren, Durchsuchen von Verzeichnissen nicht zulassen
- PWS nur in Verbindung mit einer Personal Firewall betreiben
- Default-Scripte, Beispiel-Scripte und IIS-Help aus dem direkten Serverzugriff entfernen (Verzeichnisse und Default-Dokumente umbenennen oder Alias löschen)
- Server-Scripts (CGI, PHP, ASP) nur von Alias-Verzeichnissen ausführen, Scripting nur in dafür bestimmten Verzeichnissen zulassen
- Keine Interpreter (Perl, TCL, PHP) in cgi-bin-Verzeichnissen ablegen
- Logging aller Zugriffe aktivieren
- Bei FrontPage Server-Extensions (_vti_*) auf Zugriffsrechte achten
- SSL-Verschlüsselung mit FZJ-Zertifikat einrichten (ZAM-TKI-0378)
- **Konfiguration mit MBSA überprüfen !**



IIS mit sicherer Verbindung einrichten (SSL)

1. Mit "Internet-Informationdienste – Standardwebsite – Eigenschaften – Verzeichnissicherheit – Serverzertifikat" eine Zertifikatsanforderung erstellen
2. Funktion „Serverzertifikat anfordern“ auf dem CA-Server des FZJ <http://www.fz-juelich.de/CA/x509/ca-home.htm> ausführen und den Text aus der Zertifikatsanforderung mit cut&paste in das Feld „PKCS“ einfügen. Formular ausfüllen und abschicken **Zertifikatsrequest**
3. Antragsformular ausdrucken und beim ZAM-Dispatch mit Personalausweis unterzeichnen
4. Den Text des per E-Mail oder Web erhaltenen **PKCS7-Zertifikats** zwischen BEGIN und END etwa als **servercert.p7b** auf dem Desktop ablegen
5. Mit Hilfe des IIS-Zertifikatsassistenten (siehe 1) das Zertifikat installieren
6. Zuletzt mit "Verzeichnissicherheit - Sichere Kommunikation - Bearbeiten" und "Sicheren Kanal verlangen" den ausschließlichen Zugriff über SSL (Port 443) verlangen. (Achtung: Mögliches Deadlock bei Problemen mit dem Zertifikat !)



Systemsicherung

Systemwiederherstellung (*checkpointing*)

Windows-Backup

Image-Backup mit Deploy Center



Systemwiederherstellung (Checkpointing)

- Erstellen von "Wiederherstellungspunkten" (Systemprüfpunkte, checkpoints) zum Rückgängigmachen von Systemänderungen
- Eigene Dateien (Dokumente, Emails, Favoriten etc.) werden dabei nicht gelöscht (!?), aber Vorsicht bei ausführbaren Programmen wie z.B. selbstextrahierende Archive
- Systemwiederherstellungen eines früheren Systemprüfpunkts können ihrerseits wieder rückgängig gemacht werden
- Wiederherstellungspunkte werden bei Systemänderungen (Softwareinstallation, neue Treiber) oder in längeren Zeitabständen auch automatisch vom System erstellt (Systemwiederherstellungsdienst)
- Wiederherstellungspunkte sollten **vor** jeder Installation kritischer Software auf jeden Fall mit entsprechendem Kommentar von Hand erstellt werden



Prüfen der Wiederherstellungspunkte

1. Start – Alle Programme – Zubehör – Systemprogramme – Systemwiederherstellung – einen Wiederherstellungspunkt erstellen oder Start – Hilfe und Support – Systemwiederherstellung
2. Computer zu einem früheren Zeitpunkt wiederherstellen – Weiter

letzten Checkpoint (8.Juni) und aktuelles Datum (11.Juni) überprüfen

1. Klicken Sie im Kalender auf ein in fett markiertes Datum.

Juni 2003						
Mo	Di	Mi	Do	Fr	Sa	So
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	1	2	3	4	5	6

2. Klicken Sie in der Liste auf einen Wiederherstellungspunkt.

Sonntag, 8. Juni 2003	
22:19:40	Pfingsten 2003, vor Installation NPFW.

3. Bei Bedarf "Zurück" und einen neuen Wiederherstellungspunkt erstellen



Neuen Wiederherstellungspunkt erstellen

- Im Falle, daß...

Mit der Systemwiederherstellung können Sie schädigende am Computer durchgeführte Änderungen rückgängig machen, und somit dessen frühere Einstellungen und Leistung wiederherstellen. Der Computer wird zu einem früheren Zeitpunkt (Wiederherstellungspunkt genannt) wiederhergestellt, ohne dass kürzlich bearbeitete Dateien, wie z.B. gespeicherte Dokumente, E-Mail-Nachrichten oder Verlaufslisten und Favoriten verloren gehen.

Alle von der Systemwiederherstellung vorgenommenen Änderungen können vollständig rückgängig gemacht werden.

Klicken Sie auf die Aufgabe, die durchgeführt werden soll:

- Computer zu einem früheren Zeitpunkt wiederherstellen
- Einen Wiederherstellungspunkt erstellen**

Einen Wiederherstellungspunkt erstellen

Der Computer stellt Wiederherstellungspunkte automatisch nach Zeitplänen oder vor Programminstallationen her. Sie können Wiederherstellungspunkte aber auch zu anderen Zeiten mit der Systemwiederherstellung erstellen.

Geben Sie eine Beschreibung für den Wiederherstellungspunkt im folgenden Textfeld ein. Verwenden Sie eine eindeutige Beschreibung, damit Sie sie im Fall einer erforderlichen Computerwiederherstellung sofort erkennen können.

Beschreibung des Wiederherstellungspunkts:

vor NAI Antivirus, vor Norton Personal Firewall 2003

Das heutige Datum und die aktuelle Uhrzeit werden dem Wiederherstellungspunkt automatisch hinzugefügt.

... kein geeigneter Wiederherstellungspunkt existiert

wichtig:
aussagekräftiger Kommentar !



Arbeitsplatz – RM - Eigenschaften - Systemwiederherstellung

Benötigten Speicherplatz ggf. anpassen

Partition für Arbeitsdaten

Überwachung für Arbeitsdaten, Imagebackups, Dokumente, Programmdistributionen etc. auf separater Partition oder Festplatte deaktivieren!

J.Meißburger, FZJ -ZAM

Seite 59



Übertragen von Dateien und Einstellungen

- Benutzerprofile, Eigene Dateien, Programmeinstellungen von einem Computer zu einem anderen übertragen (Ab Win95 ... XP)
- Funktioniert sinnvoll nur über Netz oder auf Wechselmedium (typisch einige 100 MB !). Persönliche Einstellungen ohne Daten ca. 50 Mbyte

- USB-Flashdisk

Direktes Kabel (verbindet die seriellen Anschlüsse des Computers)
 Heim- oder kleines Firmennetzwerk
 Ein Netzwerk ist optimal für die Übertragung einer großen Datenmenge.
 Diskette oder andere Wechselmedien
 Stellen Sie sicher, dass auf beiden Computern der gleiche Laufwerktyp vorhanden ist.
 Anderer Datenträger, z.B. austauschbares Laufwerk oder Netzlaufwerk
 Dateien und Einstellungen können auf einem Laufwerk oder in einem Ordner auf dem Computer gespeichert werden.

- Nur „Einstellungen“ oder „Auswählen einer benutzerdefinierten Liste von Dateien und Einstellungen“ auswählen
- Gegebenenfalls Dateien nach Ordner oder Dateiendung von der Übertragung ausschließen

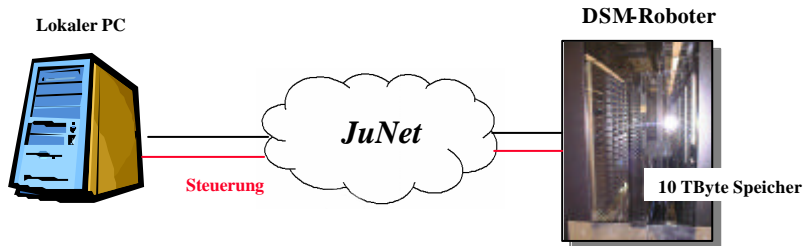
J.Meißburger, FZJ -ZAM

Seite 60



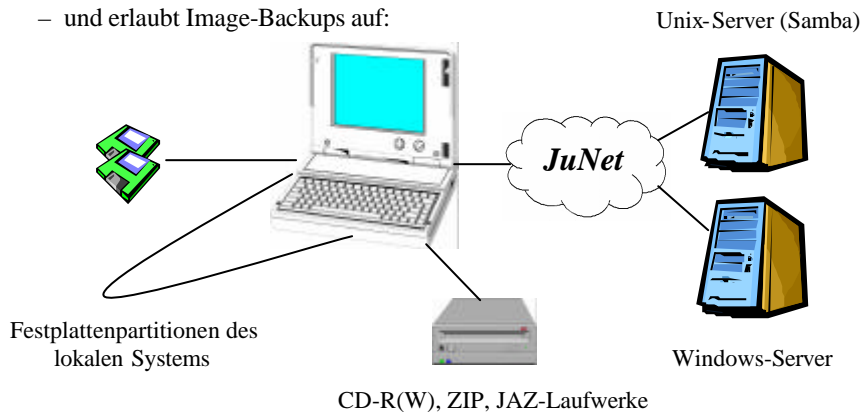
Inkrementelles Backup für Benutzerdaten im JuNet

- ADSM (Tivoli) zur regelmäßigen Sicherung von Betriebssystem-Dateien (Konfigurationsdateien) und der Benutzerdaten (incremental backup)
- Backup-Start von Hand, durch lokalen Taskplaner oder fremdgesteuert vom ADSM-Server (L.Wollschläger, 6420)
- **Achtung bei 10 Mb Thinwire-Netzanschluß: Unbedingt mit lokaler Kompression arbeiten, sonst Netzüberlastung!!**



DriveImage / DeployCenter ZAM-IB-2001-02

- Disk-Imaging-Software
 - läuft vollständig von zwei Disketten unter einem stand-alone-Betriebssystem (DOS) oder gestartet von Windows
 - und erlaubt Image-Backups auf:





Kleine Helfer für die Sicherheit

Starke Dateiverschlüsselung

Secure Shell

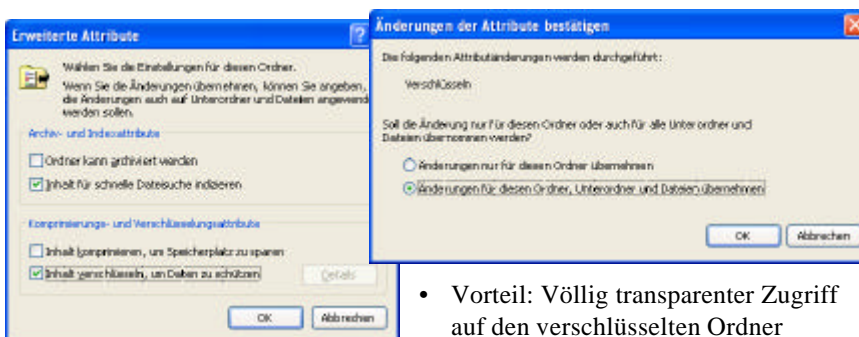
Task-und Prozeßanalyse

IP-Portüberwachung



Verschlüsselung von Ordnerinhalten

- Ordner – RM – Eigenschaften – Erweitert
- Inhalt verschlüsseln, Änderungen für Ordner übernehmen
- Vorsicht: Bei Verlust des zugehörigen privaten Schlüssels (z.B. auf einem anderen Computer) geht der Zugriff auf den Ordner verloren !

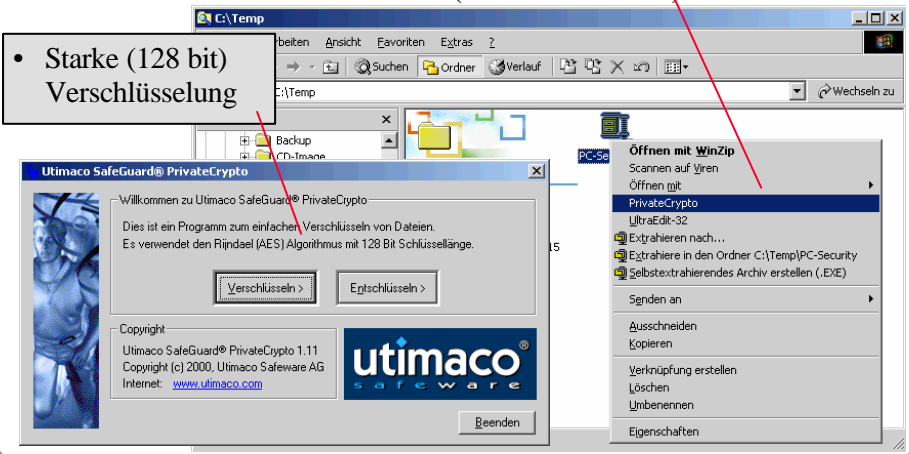


- Vorteil: Völlig transparenter Zugriff auf den verschlüsselten Ordner



Dateiverschlüsselung mit Utimaco SafeGuard® PrivateCrypto

- Einfach zu benutzende Verschlüsselung von Ordnern und Dateien durch Zusatz-funktion im Kontext-Menü (Rechte Maustaste)



- Starke (128 bit) Verschlüsselung



Secure Shell: Sicherer Zugang zu Unix-Systemen

- Für Mitarbeiter des FZJ frei verfügbare Software für den voll verschlüsselten Zugang zu Unix-Systemen. Siehe:
 - <http://www.fz-juelich.de/zam/net/security/software/ssh/pc>
- SSH-Win
 - VT-kompatibler Terminalzugang mit ssh V1+2 für Window
 - Komfortabler Filetransfer wie im Windows-Explorer (Drag&Drop)
 - Konstenpflichtiger SSH V2-Server für Windows
- SSH-DOS
 - VT-kompatibler Terminalzugang mit ssh V1+2 für DOS
 - Secure File Copy
- Cygwin
 - Frei verfügbare, sehr leistungsfähige Unix-Emulation mit vollständiger Open-SSH-Implementierung (Client und Server)
 - Siehe ZAM -TKI-0375



Nützliche Freeware

Siehe auch Heft-CDs von PC-Welt, c't, iX, Computer-Bild etc.



RegCleaner zur Überprüfung und Bereinigung der Registry



Microsoft: Start – Ausführen – msconfig

Zur Steuerung des automatischen Starts von Diensten und Programmen



TCPView zeigt detailliert alle offenen IP-Verbindungen, Dienste und Ports



ClearProg dient zum Löschen temporärer Dateien (Privacy !)



Process Explorer

und zeigen alle laufenden Tasks mit den zugehöriger Prozeßinformation wie Quelldatei, Handles, DLL's, Ownerships....



Process Viewer



Zusammenfassung

- Aktuelle Betriebssysteme und Patches einspielen (Microsoft Tools benutzen) <http://v4.windowsupdate.microsoft.com/de/default.asp>)
- Regelmäßiges Sichern des Betriebssystems und wichtiger Benutzerdaten, Start/Notfalldiskette erstellen und testen (**PowerQuest ImageCenter 5.01**)
- Abschalten nicht benutzter Dienste und Protokolle (nur TCP/IP verwenden!)
- Paßwortgeschützte (verschlüsselte) Benutzerauthentisierung. **Keine anonymen Accounts**. Paßwortschutz für Freigaben („Shares“). Freigaben "verstecken"
- Nutzung eingebauter Sicherheitsmechanismen in Windows-Applikationen (Internet-Explorer, Office-Programme, E-Mail)
- Die **Einrichtung eines aktuellen Virenschutzprogramms** vor allem für E-Mail und File Download (**F-Prot und NAI Virusscan**)
- Einrichtung eines **persönlichen Firewalls** (Microsoft Verbindungsfirewall, [besser Norton Personal Firewall](#)) zur Steuerung und Kontrolle des IP-Verkehrs